2013 International Siberian Conference on Control and Communications, SIBCON 2013 - Proceedings, 2013

Experimental verification of possibility of secret encryption keys distribution with a phase method in a multipath environment

Smolyakov A., Sulimov A., Karpov A., Sherstyukov O.
Kazan Federal University, 420008, Kremlevskaya 18, Kazan, Russia

Abstract

The paper addresses a problem of creating a system for generation and distribution of shared secret encryption key based on the physical properties of multipath radio propagation. A multipath radio channel with reciprocal properties is considered as a source of shared randomness, as the phase of the passed through multipath environment signal becomes unpredictable. The paper presents the results of experimental verification of feasibility of the generation and distribution of shared secret encryption key based on measurements of random phase of a multipath signal. The problem of checking the symmetry of instances of the generated shared encryption key through the exchange of cyclic redundancy codes is considered. The probability of a bit asymmetry of the generated from the experimental phase measurements instances of the shared encryption key is evaluated. The effectiveness of encryption key distribution process is estimated. © 2013 IEEE.

http://dx.doi.org/10.1109/SIBCON.2013.6693653

Keywords

channel reciprocity, data rate of encryption keys distribution, effectiveness of encryption keys distribution, Encryption keys distribution, error bit rate, multipath radio propagation, randomness of carrier phase, shared randomness, theoretic security